AMENDMENTS TO THE CLAIMS

1(original). A method of electronically verifying that a person possessing a security device is who the person claims to be, comprising:

sending a message by said security device associated with the person whose identity is to be verified, said message including said person's public key number;

receiving said message by a host, said host encrypting a random message using said public key number and sending said public key number encrypted message to said security device;

said security device decrypting said public key number encrypted random message using said person's private key number and sending said decrypted random message to said host; and

said host comparing the decrypted random message sent by the security device with the random message previously encrypted by said host with said public key number to verify the identity of the person.

2(original). A method in accordance with Claim 1 wherein said security device is a computer with associated security hardware having said person's private key number programmed therein.

3(original). A method in accordance with Claim 1 wherein said security device is a laptop computer with associated security hardware having said person's private key number programmed therein.

4(original). A method in accordance with Claim 2 wherein said security hardware

includes a one time programmable macroprocessor.

5(original). A method in accordance with Claim 3 wherein said security hardware includes a one time programmable microprocessor.

6(original). A method in accordance with Claim 2 wherein said security hardware includes a read only memory for storing said person's private key number.

7(original). A method in accordance with Claim 3 wherein said security hardware includes a read only memory for storing said person's private key number.

8(original). A method in accordance with Claim 1 wherein said security device is a computer provided with associated security software having said person's private key number programmed therein.

9(original). A method in accordance with Claim 1 wherein said security device is a laptop computer provided with associated security software having said person's private key number programmed therein.

10(original). A method in accordance with Claim 2 wherein said security hardware is insertable and removable in a drive of said computer.

11(original). A method in accordance with Claim 3 wherein said security hardware is insertable and removable in a drive of said laptop computer.

12(original). A method in accordance with Claim 1 wherein said security device is a badge or identification card with associated security hardware having said person's private key number programmed therein.

13(original). A method in accordance with Claim 1 wherein said security device is a car key with associated security hardware having said person's private key number

programmed therein.

14(original). A method in accordance with Claim 2 wherein said security hardware communicates with a computer by an infrared link.

15(original). A method in accordance with Claim 2 wherein said security hardware communicates with a computer by a radio frequency link.

16(original). A method in accordance with Claim 3 wherein said security hardware communicates with a laptop computer by an infrared link.

17(original). A method in accordance with Claim 3 wherein said security hardware communicates with a laptop computer by a radio frequency link.

18(original). A method in accordance with Claim 1 wherein said host first sends a query to said security device as to its identity before said security device sends a message which includes said person's public key number.

19(original). A method in accordance with Claim 1 wherein the method of electronically verifying is repeated during a session on which said security device is logged-on to said host.

20(original). A method in accordance with Claim 19 wherein said repeated verification is invisible to said person possessing said security device.

21(original). A method in accordance with Claim 19 wherein said host compartmentalizes data requiring a verification for each data compartment.

22(original). Apparatus for enabling electronic identification of a person, comprising:

means for permanently storing a corresponding private key number and a public key

number assigned to said person;

means for sending said public key number to a host seeking to verify the identity of said person;

means for receiving from said host a random message encrypted with said public key number;

means for decrypting said random message encrypted with said public key number; and

means for sending said decrypted random message to said host for comparison to said random message previously encrypted with said public key number to verify the identity of said person.

23(original). Apparatus in accordance with Claim 22 including means at said host for generating a random message.

24(original). Apparatus in accordance with Claim 23 including means at said host for encrypting said random message.

25(original). Apparatus in accordance with Claim 23 wherein said random message is a random number.

26(original). Apparatus in accordance with Claim 24 wherein said means at said host for encrypting includes use of the RSA algorithm.

27(original). Apparatus in accordance with Claim 22 wherein said means for decrypting said random message includes use of the RSA algorithm.

28(original). Apparatus in accordance with Claim 22 wherein said means for permanently storing is comprised of a one time programmable microprocessor.

29(original). Apparatus is accordance with Claim 22 wherein said means for permanently storing comprises a read only memory.

30(original). Apparatus in accordance with Claim 22 wherein said apparatus is contained on security hardware which communicates with a computer.

31(original). Apparatus in accordance with Claim 22 wherein said computer is a laptop computer.

32(original). Apparatus in accordance with Claim 30 wherein said security hardware communicates with said computer by an infrared link.

33(original). Apparatus in accordance with Claim 30 wherein said security hardware communicates with said computer by a radio frequency link.

34(original). Apparatus in accordance with Claim 22 wherein said apparatus is mounted on a badge.

35(original). Apparatus in accordance with Claim 22 wherein said apparatus is mounted on a card for use as a car key.

36(original). Apparatus in accordance with Claim 22 wherein said apparatus is mounted on a card for use as a financial transaction card.

37(original). Apparatus in accordance with Claim 22 wherein said apparatus is mounted on an identification card.

38(new). An apparatus, comprising:

a self contained stand alone security device which contains a memory for permanently storing a public key number and a corresponding private key number, transmitter means, receiver means and decryption means;

said permanent memory storing a corresponding private key number and a public key number assigned to a person to be identified by said stand alone security device;

said transmitter means for sending said public key number to a host seeking to verify an identity of said person;

receiver means for receiving from said host a random message encrypted with said public key number;

said decryption means being used for decrypting said random message encrypted with said public key number using said private key number from said permanent memory;

said transmitter means for sending said decrypted random message to said host for comparison to said random message previously encrypted with said public key number to verify the identity of said person; and

wherein said apparatus functions as an admission control device and wherein said verification of the identity of the person in accordance with the foregoing steps may be repeated throughout a period of admission.